REMARKS/ARGUMENTS

This Amendment is being filed in response to the outstanding Office Action dated February 27, 2004 in which the Examiner again rejected claims 1-6, and 8-24, all of the claims, currently pending in the subject Application.

Applicant notes with appreciation the opportunity to discuss the subject application with the Examiner via telephonic interview on March 31, 2004. A copy of the Interview Summary issued by the Examiner is attached hereto as Exhibit A.

During the telephonic interview, Applicant's representative explained that an inventive feature of the claims is that a purchaser identifier could be used to initiate purchases with a web-based merchant without needing to input or transmit the purchaser's payment data, such as credit/debit card numbers. In addition, Applicant's representative explained that a further inventive feature of the claims is that the purchaser identifier is inextricably linked to the purchaser's pre-stored delivery data that cannot be modified without rendering the purchaser identifier inoperable.

These claimed features are novel and non-obvious over present electronic purchase systems, such as is described in Lewis et al., U.S. Patent No. 6,233,565, and Egendorf, U.S. Patent No. 6,188,994, because (i) no financially sensitive information is transmitted to third party merchants to make purchases and (ii) even if the purchaser identifier is stolen, the linked delivery data cannot be changed thereby preventing shipment of goods to alternate delivery addresses.

Applicant has amended independent claims 1, 14, and 17 to more clearly define the above-referenced inventive features. Claim 25 is newly presented.

///

///

///

///

I. REJECTIONS UNDER 35 U.S.C. § 103(A)

A. LEWIS ET AL., U.S. PATENT NO. 6,233,565 IN COMBINATION WITH EDWARDS AND WALKER, ET AL., U.S. PATENT NO. 5,794,207.

1. Lewis Fails To Teach Or Suggest The Features Of Claims 1, 14, and 17, As Amended.

In forming this rejection, the Examiner maintains the prior rejection based on Lewis; namely, that Lewis teaches "disabling the purchaser identifier (col. 3, lines 38-42) in response to a fraud," but does not teach disabling the purchaser identifier in response to "a specific fraud such as the delivery data associated with a particular purchaser identifier". Despite the Examiner's concession that Lewis fails to teach linking delivery data with a purchaser identifier, the Examiner asserts the following:

> [I]t would have been obvious to one of ordinary skill in the art that such a particular fraud detection measure would have constantly been monitored in the system of Lewis et al. because it has been known that hackers or thieves usually perform this type of fraud by having items or goods which they did not purchase or pay for being delivered at their desired address.

See Feb. 27th Office Action, p.3. Applicant submits that Lewis' general fraud detection measures using primarily complex encryption techniques neither teaches nor suggests the system and method of the present claims.

a. Lewis Is Not Analogous To The Present Invention And Fails To Teach Or Suggest Several Elements Of The Subject Claims.

Lewis does not teach or suggest several features of the processing system of independent claims 1, 14, 17, 20, 22, and 25, and even if combined with Edwards and Walker cannot render said claims obvious.

i. *Lewis is directed to a non-analogous type of purchasing system and employs a wholly different approach to fraud prevention, as compared to the subject claims, as amended.*

Lewis describes an electronic postage system that works in conjunction with Postal Security Device ("PSD") software residing on a Remote Service Provider ("RSP") server. The system of Lewis is very specialized and designed to process the purchase of postage from a specified postal service, such as the U.S. Postal Service ("USPS"). Because postal services employ specialized regulations and specifications, the system of Lewis was designed to comply with these specialized set of regulations and specifications. For example, Lewis states that the USPS uses the Information Based Indicia Program ("IBIP"). See Lewis, col. 1, lines 50-62. Although it is acknowledged that the system of Lewis could be modified to comply with the specific regulations of other postal service entities in Europe or Canada, for example, the Lewis system nevertheless is designed to permit postage purchases from a specific postal entity, such as the USPS, using specialized rules, such as IBIP. The Lewis system, therefore is not analogous to the systems and methods of the present claims.

In particular, in Lewis, the user must download specialized software that permits the user to communicate with the RSP 4, as follows:

> User 2n makes a purchase through a proprietary connection over the Internet 30 using the appropriate IP address as provided by the downloaded client software to connect with the RSP's Internet transaction server 180, utilizing a suitable form of payment, such as credit cards, or checks.

See Lewis, col. 12 lines 14-20. The postage purchasing system of Lewis would not be suitable as a general merchant purchasing system due to the specialized nature of Lewis' communications and security system. As will become evident from the following discussion, the specialized client software and RSP transaction server 180 operates in a wholly different manner from the systems and methods of the present claims.

ii. *Lewis teaches away from the systems and methods of the present claims in that Lewis requires transmission of payment information via the Internet.*

Lewis fails to disclose, teach or suggest the claimed feature of "us[ing] the payment data to pay for the purchased goods or services without exposing the payment data to the merchant." In Lewis, in order to purchase postage, a "suitable form of payment, such as credit cards, or checks" is required to be transmitted to the RSP's transaction server 180. See id. Specifically, Lewis describes the purchase request, as follows:

> ***The customer then initiates transmission of all of the purchase information (e.g., addresses, purchase amount, and credit/check information) via the Internet 30 to the web server 150, which passes the transaction request to the transaction server 180.*** When the Submit radio button is pressed, all customer information is digitally signed and encrypted and packaged with the purchase amount.... Because the transmission has the appropriate IP address for the transaction server 180 it will be directed by web server 150 through the firewall 160 to transaction server 180, where the transaction will be executed.

See Lewis, col. 16 lines 18-20 (emphasis added). It is clear, therefore, that in order to pay for postage in the Lewis system (except where a check is used) a user must transmit their credit/debit card number to the transaction server 180 over the Internet. This is confirmed again in Lewis at col. 14, lines 25-42, wherein it states that the RC2 symmetric encryption "will be used to protect the nature of the purchase/refund request, which may include credit card information." See also Lewis, col. 16, lines 5-22. Again at col. 17, lines 4-15 of Lewis describes the transmission of credit card numbers over the Internet:

> Credit card requests are transmitted to the web server 150 by the client, forwarded to the transaction server 180, and then to a payment server 190, a credit authorization server 400, and to a remote credit bureau 9 such as First Data Merchant Services ("FDMS").

By virtue of its chosen method of operation, the Lewis system is subject to potential interception of sensitive and valuable credit/debit card numbers. Lewis attempts to solve this problem by

using encryption of the data transmission that contains the financially sensitive data, which is entirely different from the approach presented by the present invention.[1]

Lewis, thus, fails to disclose, teach or suggest the claimed feature of "us[ing] the payment data to pay for the purchased goods or services without exposing the payment data to the merchant."

iii. *Lewis fails to disclose, teach or suggest use of a "purchaser identifier" in lieu of credit/debit card numbers to make purchases with various merchants.*

The systems and methods of claims 1, 14, 17, 20, 22 and 25, provide a user/purchaser with a purchaser identifier, which includes no financially usable information (e.g., credit card numbers or the like) and cannot be used to make purchases with any system other than the transaction processing system of the claims, to make purchases with any online merchant system, such as, by way of example, Amazon.com or CircuitCity.com.

With respect to the lack of a teaching or suggestion of a purchaser identifier, in Lewis, the user is identified through interaction of the downloaded client software and the transaction server 180. Lewis, therefore, neither teaches nor suggests use of a purchaser identifier that is an alpha-numeric code that is not the purchaser's credit or debit card number or other financially sensitive information. In contrast, Lewis requires the transmission of financially sensitive information each time a purchase is to be made.

Moreover, Lewis describes an initial registration procedure in which the user enters certain preliminary information. See Lewis, col. 11, lines 13-63. This information may include an address for the user. Id. Lewis, however, makes no teaching or suggestion that this address will be inextricably linked to a specific purchaser identifier or that the shipping address cannot

[1] For the sake of clarification, Applicant is not arguing that encryption methods cannot be used within the scope of the present invention, but rather that the present invention achieves its fraud protection via a novel approach of using a purchaser identifier inextricably linked to pre-stored delivery addresses that cannot be changes without rendering the purchaser identifier inoperable.

be changed without disabling the purchasing system, and specifically the purchaser identifier. In Lewis the only thing being purchased is a monetary postage value. The postage value is not delivered to the customer, but rather is stored at the RSP server 4 in a descending register account for the customer. The addresses discussed in Lewis refer to mail delivery addresses used by the system of Lewis to calculate the amount of postage necessary to send a customer's mail. In contrast to Lewis where there are no goods or services to be delivered to the customer (only postage stored at a remote server), the claims of the present invention are directed to a system in which purchased goods or services will be physically or electronically delivered to a pre-stored customer's delivery address. Thus, the system of Lewis is entirely non-analogous to the present invention and fails to disclose, teach, or suggest the features of claim 1, as amended, of using a purchaser identifier that is linked to a delivery address.

Thus, Lewis fails to disclose, teach or suggest the purchaser identifier of claim 1, as amended, and further fails to disclose, teach or suggest linking the purchaser identifier to a delivery address that cannot be changed. Moreover, Lewis teaches transmitting credit card information or the like over the Internet to make postage purchase, whereas the claims of the present invention, as amended, set forth that no such financial information is transmitted across the Internet.

As such, the claims, as amended, present a novel online purchase processing system that (1) reduces the risk that a credit number might be stolen or compromised by creating a secure third party entity to hold consumer's credit cards and deliver only purchase authorizations and pre-stored delivery addresses to merchants when a purchase request is received, and (2) reduces the ability of a thief to use a stolen consumer identifier, such as a pin number, by limiting delivery of the purchased goods or services to only pre-stored delivery addresses.

Applicant, therefore, respectfully submits that the claims 1-6 and 8-19 are allowable as amended over the Lewis reference.

2. **Edwards And Walker Do Not Teach Or Suggest Inextricably Linking Delivery Data To A Purchaser Identifier.**

The Examiner concedes that Lewis does not teach the claimed feature "wherein the purchaser identifier is generated by the processing system during storage of the delivery data in the purchaser account database and is inextricably linked to the delivery data such that any change or attempted change to the delivery data will render the purchaser identifier inoperable". Nevertheless, the Examiner cites to the Edwards and Walker references as teaching this feature. Applicant submits that neither Edwards nor Walker teach or suggest the feature of inextricably linking a delivery address to a purchaser identifier to be used to make purchases.

a. Edwards Is Not Analogous To And Should Not Be Combined With Lewis.

Edwards is an article that advises travel agents on how to avoid becoming credit card fraud victims by verifying a credit card holder's address using an address verification system. Edwards does not present an electronic purchasing system, but rather is directed to the purchase of airline tickets over the phone. Edwards describes a scenario where the consumer gives the travel agent a credit card number and a billing address. The travel agent uses an address verification system to attempt to match the address to the card number. If the billing address does not match the address stored by the credit card company, Edwards advises the travel agent to deny the transaction. Because Edwards is not directed to the field of electronic commerce over the Internet, there would be no motivation to combine Edwards with Lewis.

b. Edwards Fails To Disclose, Teach Or Suggest The Feature Of Inextricably Linking A Delivery Address To A Purchaser Identifier.

Even if Edwards is combined with Lewis, as suggest by the Examiner, the combination would not render the claims, as amended, obvious. Notwithstanding the numerous deficiencies of Lewis as described above, Edwards fails to teach or suggest inextricably linking the delivery data to the purchaser identifier such that any change or attempted change to the delivery data will render the purchaser identifier inoperable. First, Edwards makes no teaching of a purchaser

identifier that is different from any financially sensitive information, such as a credit card number. In contrast, the purchaser's credit card number is given directly to the merchant, which is exactly opposite to the systems and methods of the present claims.

Second, Edwards only crosschecks a billing address with the stored address of the credit card consumer, and makes no mention of any delivery address for the tickets. If the billing address matched (such as in the case where a hacker intercepted an online purchase including both a consumer's credit card number and billing address), the hacker would likely be able to send the airline tickets to any other shipping address. This is because in heretofore known electronic commerce systems, the ability to change delivery addresses was viewed as being advantageous so that the purchaser could ship the goods to any desired address. As such, if the purchaser desired to send someone a gift, the purchaser could easily do so by changing the shipping address to that of the person receiving the gift. The claims of the present application, however, set forth an entirely opposite approach where the purchaser is not given the option to change the delivery addresses, so that the incentive for a thief to steal the purchaser identifier is reduced. In such a system, for instance, even if a consumer's purchaser identifier is stolen, a potential thief would have no incentive to use the purchaser identifier because the thief could not change the pre-stored delivery addresses without rendering unusable the purchaser identifier. Thus, even if the thief purchased goods, the goods would be delivered to the account owner's pre-stored delivery address and the account owner would quickly recognize the fraud and have an opportunity to take action.

Therefore, because Edwards fails to teach or suggest a purchaser identifier and the linking of the purchaser identifier to a delivery address, Edwards fails to render the claims obvious even if combined with Lewis.

c. Walker Fails To Teach Or Suggest Inextricably Linking The Delivery Data To The Purchaser Identifier Such That Any Change Or Attempted

Change To The Delivery Data Will Render The Purchaser Identifier Inoperable.

While Walker is directed to an electronic commerce system, Walker also fails to teach or suggest inextricably linking the delivery data to the purchaser identifier such that any change or attempted change to the delivery data will render the purchaser identifier inoperable.

In the passages of Walker identified by the Examiner, namely col. 8:66-9:30 and 13:1-19, Walker describes usage of a unique ID number to identify the buyer. Walker, however, does not teach or suggest inextricably linking the ID number to a delivery address for the delivery of goods or services. Moreover, Walker fails to teach or suggest that a change or attempted change in the delivery address would result in the ID number being rendered inoperable. In contrast, Walker only describes storing the buyer's address, which is presumably the buyer's home address, but does not otherwise discuss storing or linking a delivery address to the ID number. Indeed, in Walker at col. 12, lines 31-49, the exchange of goods between buyer and seller are described. There is no mention in this section that the goods are required to be delivered to a pre-stored delivery address because the delivery address is linked to the ID number. Thus, Walker fails to teach or suggest the claimed feature of inextricably linking the delivery data to the purchaser identifier such that any change or attempted change to the delivery data will render the purchaser identifier inoperable.

As such, neither of the combinations suggested by the Examiner in rejecting the claims, even if such combination was, which it is not, render the claims obvious. In light of the above arguments and amendments to the claims, Applicant respectfully requests that the Examiner withdraw the rejection.

B. **REJECTIONS UNDER 35 U.S.C. § 103(A) OVER EGENDORF, U.S. PATENT NO. 6,188,994 IN VIEW OF LEWIS ET AL., U.S. PATENT NO. 6,233,565, EDWARDS AND WALKER, ET AL., U.S. PATENT NO. 5,794,207.**

The Examiner also rejected claims 20-21 over U.S. Patent No. 6,188,994 to Egendorf in view of Edwards and Walker, and claims 22-24 as being obvious over Egendorf in view of Lewis, Edwards, and Walker.

With respect to these rejections, the Examiner concedes that Egendorf does not teach or suggest the feature wherein "once the secure consumer account is established by the consumer and the unique customer identifier is assigned to the customer account, the at least one delivery address associated with the unique consumer identifier cannot be changed without causing the unique consumer identifier to be disabled". Nevertheless, the Examiner asserts that it would have been obvious to prevent a purchaser from changing the delivery address in order to prevent intruders from tangling with the purchasing system.

Egendorf, however, includes no motivation to include a purchaser identifier that is inextricably linked to at least one delivery address as is set forth in the claims, as amended. In fact, Egendorf teaches away from the present claims in so far as Egendorf teaches that during the course of making a purchase, the means of delivery of the goods or service will be established. Thus, there is no requirement in Egendorf that the delivery address be prestored and inextricably linked to a purchaser identifier. In contrast, in the system of Egendorf, a purchaser will have the opportunity to specify any delivery address that the purchaser desires at the time of purchase therefore subjecting the system to potential fraudulent transactions made by thieves who have stolen the consumer's identifier. Thus, Egendorf teaches away from the system of the present claims and, therefore, contains no motivation to a person of skill in the art to modify Egendorf to include the features of claims 20-24.

With respect to the proposed combination of Egendorf with Lewis, Edwards, and Walker, Applicant refers to the arguments set forth above. Even if the proposed combinations are made, none of the references teaches or suggests the claimed feature of inextricably linking the delivery data to the purchaser identifier such that any change or attempted change to the delivery data will

render the purchaser identifier inoperable, as well as other features highlighted above. For this reason, Applicant submits that claims 20-24 are allowable over the cited references.

II. CONCLUSION

Applicant has made a diligent effort to place the Application in condition for allowance and respectfully submits that claims 1-6 and 8-25 in light of the amendments and arguments set forth above are in condition for immediate allowance. Consequently, if the Examiner cannot issue an immediate allowance of the present application, the Examiner is respectfully requested to contact the undersigned attorney to discuss the outstanding issues.

Applicant authorizes the U.S. Patent Office to charge any new and additional fees or charges, including any fees for a petition for an extension of time, to Deposit Account No. 19-4709, if necessary.

Respectfully submitted,

By: _____

Richard Eskew, Reg. No. 48,874
for Steven B. Pokotilow
Registration No. 26,405
Attorney For Applicant
Stroock & Stroock & Lavan LLP
180 Maiden Lane
New York, New York 10038-4982
(212) 806-5400